

11-03-00

A

Please type a plus sign (+) inside this box → ☐

PTO/SB/05 (4/98) Approved for use through 09/30/2000 OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No.	15-0231
First Inventor or Application Identifier	Kenneth W. Aull
Title	CHAIN OF TRUST PROCESSING
Express Mail Label No.	EK745231842US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

- ☒ * Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)
- ☒ Specification [Total Pages 32] 1
(preferred arrangement set forth below)
 - Descriptive title of the invention
 - Cross References to Related Applications
 - Statement Regarding Fed sponsored R & D
 - Reference to Microfiche Appendix
 - Background of the invention
 - Brief Summary of the invention
 - Brief Description of the Drawings (if filed)
 - Detailed Description
 - Claim(s)
 - Abstract of the Disclosure
- ☒ Drawing(s) (35 U.S.C. 113) [Total Sheets 7] 1
- Oath or Declaration [Total Pages 1] 1
 - ☐ Newly executed (original or copy)
 - ☐ Copy from a prior application (37 C.F.R. § 1.63(d))
(for continuation/divisional with Box 16 completed)
 - ☐ **DELETION OF INVENTOR(S)**
Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

- ☐ Microfiche Computer Program (Appendix)
- Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
 - ☐ Computer Readable Copy
 - ☐ Paper Copy (identical to computer copy)
 - ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

- ☒ Assignment Papers (cover sheet & document(s))
- ☒ 37 C.F.R. § 3.73(b) Statement (when there is an assignee) ☒ Power of Attorney
- ☐ English Translation Document (if applicable)
- ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
- ☐ Preliminary Amendment
- ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
- ☐ * Small Entity Statement(s) ☐ Statement filed in prior application (PTO/SB/09-12) ☐ Status still proper and desired
- ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed)
- ☒ Other: Declaration-Unexecuted Copy

* NOTE FOR ITEMS 1 & 13 IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:

<input type="checkbox"/> Continuation	<input type="checkbox"/> Divisional	<input type="checkbox"/> Continuation-in-part (CIP)	of prior application No. _____
Prior application information: Examiner _____		Group / Art Unit: _____	

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

<input type="checkbox"/> Customer Number or Bar Code Label	(Insert Customer No. or Attach bar code label here)	or <input checked="" type="checkbox"/> Correspondence address below
--	---	---

Name	Michael S. Yatsko				
	TRW Inc.				
Address	Law Dept. One Space Park, Bldg. E2/6051				
City	Redondo Beach	State	CA	Zip Code	90245
Country	U.S.A.	Telephone	310-812-4910	Fax	310-812-2687

Name (Print/Type)	Michael Yatsko	Registration No. (Attorney/Agent)	28,135
Signature	Michael S. Yatsko	Date	11/01/00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

FEE TRANSMITTAL

for FY 2000

Patent fees are subject to annual revision.
Small Entity payments must be supported by a small entity statement,
otherwise large entity fees must be paid See Forms PTO/SB/09-12.
See 37 C.F.R. §§ 1.27 and 1.28.

TOTAL AMOUNT OF PAYMENT (\$956.00)

Complete if Known

Application Number
Filing Date November 1, 2000
First Named Inventor Kenneth W. Aull
Examiner Name Unassigned
Group / Art Unit N/A
Attorney Docket No. 15-0231

METHOD OF PAYMENT (check one)

1. ☒ The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to.

Deposit Account Number 20-1515

Deposit Account Name TRW Inc.

☒ Charge Any Additional Fee Required Under 37 CFR §§ 1.16 and 1.17

2. ☐ Payment Enclosed:
☐ Check ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description	Fee Paid
101 690	201 345	Utility filing fee	710.00
106 310	206 155	Design filing fee	
107 480	207 240	Plant filing fee	
108 690	208 345	Reissue filing fee	
114 150	214 75	Provisional filing fee	

SUBTOTAL (1) (\$ 710.00)

2. EXTRA CLAIM FEES

Total Claims	Extra Claims	Fee from below	Fee Paid
27	-20** = 7	18	126
4	-3** = 1	80	80
Multiple Dependent			0

**or number previously paid, if greater; For Reissues, see below

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description	Fee Paid
103 18	203 9	Claims in excess of 20	
102 78	202 39	Independent claims in excess of 3	
104 260	204 130	Multiple dependent claim, if not paid	
109 78	209 39	** Reissue independent claims over original patent	
110 18	210 9	** Reissue claims in excess of 20 and over original patent	

SUBTOTAL (2) (\$ 206.00)

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description	Fee Paid
105 130	205 65	Surcharge - late filing fee or oath	0.00
127 50	227 25	Surcharge - late provisional filing fee or cover sheet.	0.00
139 130	139 130	Non-English specification	0.00
147 2,520	147 2,520	For filing a request for reexamination	0.00
112 920*	112 920*	Requesting publication of SIR prior to Examiner action	0.00
113 1,840*	113 1,840*	Requesting publication of SIR after Examiner action	0.00
115 110	215 55	Extension for reply within first month	0.00
116 380	216 190	Extension for reply within second month	0.00
117 870	217 435	Extension for reply within third month	0.00
118 1,360	218 680	Extension for reply within fourth month	0.00
128 1,850	228 925	Extension for reply within fifth month	0.00
119 300	219 150	Notice of Appeal	0.00
120 300	220 150	Filing a brief in support of an appeal	0.00
121 260	221 130	Request for oral hearing	0.00
138 1,510	138 1,510	Petition to institute a public use proceeding	0.00
140 110	240 55	Petition to revive - unavoidable	0.00
141 1,210	241 605	Petition to revive - unintentional	0.00
142 1,210	242 605	Utility issue fee (or reissue)	0.00
143 430	243 215	Design issue fee	0.00
144 580	244 290	Plant issue fee	0.00
122 130	122 130	Petitions to the Commissioner	0.00
123 50	123 50	Petitions related to provisional applications	0.00
126 240	126 240	Submission of Information Disclosure Stmt	0.00
581 40	581 40	Recording each patent assignment per property (times number of properties)	40.00
146 690	246 345	Filing a submission after final rejection (37 CFR § 1.129(a))	0.00
149 690	249 345	For each additional invention to be examined (37 CFR § 1.129(b))	0.00
Other fee (specify)			0.00
Other fee (specify)			0.00

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) (\$ 40.00)

SUBMITTED BY

Name (Print/Type) Michael S. Yatsko
Signature Michael S. Yatsko

Registration No. 28,135
(Attorney/Agent)

Complete (if applicable)

Telephone 310-812-4910
Date 11/6/00

WARNING:

Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

"Express Mail Mailing Label Number"

EK745231842US 11/01/00

Date of Deposit
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR §1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Lorna L. Schott

(Typed or printed name of person mailing)

(Signature of person mailing)

CHAIN OF TRUST PROCESSING

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of Provisional
5 Application Serial No. 60/229,336, filed in the U.S. Patent
and Trademark Office on September 1, 2000, the contents of
which are expressly incorporated by reference herein.

BACKGROUND OF THE INVENTION

Field of the Invention

10 The present invention relates to digital certificates in
a PKI (Public Key Infrastructure). More particularly, the
present invention relates to using a first certificate of a
user to authenticate the user's identity in subsequent
certificate processing.

15 Description of the Related Art

A PKI is a set of policies, procedures, and software that
permit an organization to generate, issue, and manage

public/private cryptographic keys in a manner that allows users to reliably determine the identity of the owner of each public/private key pair. The key components of a PKI include:

(1) a mechanism for reliably conveying the identity of a key pair's owner to the end user; (2) software applications for generating and managing key pairs that support this mechanism; (3) a set of procedures for generating and revoking key pairs that ensures that the identity of the owner can be reliably determined; and (4) a set of policies defining who may obtain public/private key pairs and identifying how each pair may be used.

As to component (1) of a PKI, most PKIs establish that the user owns a key pair by using an electronic document called a digital certificate. Digital certificates contain information identifying the owner of the key pair, the public component of the pair, and the period of time for which the certificate is valid. The digital certificate also identifies technical information about the key itself, such as the algorithm used to generate the key and the key length.

Certificates are generated by organizations that are responsible for verifying the identity of individuals, or in some instances, other organizations to which certificates are being issued. The identity of the certifying organization, referred to as a certificate authority, is recorded in each certificate, which is then signed using a private key known

only to the certificate authority itself. This allows users to verify both the integrity of the certificate and the identity of the authority that issued it.

Certificate authorities generally employ any of a number
5 of different commercially available software products to manage the creation, renewal, and revocation of certificates. These Certificate Management Systems (CMS) take information obtained through the user registration process, create a certificate, and sign it with the certificate authority's
10 private key. The applicable CMS software maintains a database of all of the certificates that it has issued, and their statuses. The CMS is also responsible for revoking certificates, and for publishing a certificate revocation list that identifies the date on which each certificate was
15 revoked, and the reason for the revocation. This information allows relying users (that is, those individuals or systems that are performing encryption or signature verification actions based on certificates) to review the status of a certificate, to assess its usability. A list of distribution
20 points from which the CRL can be obtained are identified in the certificate itself.

In issuing a certificate, a certificate authority is stating that it has verified that the public key that appears in the certificate (and, by extension, the corresponding
25 private key) belongs to the individual listed in the

certificate. The integrity with which the registration process operates is therefore of great importance. The process must provide mechanisms for reliably identifying an individual and for verifying that the public key listed in the certificate
5 belongs to that individual. Equally important, the certificate authority must provide procedures for revoking certificates in the event that the private key is compromised. A compromised private key calls into question the entire basis for trusting a certificate, since more than one individual may be using
10 that private key to sign documents, or more than one individual may be able to decrypt documents encrypted using the corresponding public key.

Relying individuals and organizations must have a clear understanding of their certificate authority's operation
15 processes. As a result, most certificate authorities publish a Certificate Practice Statement (CPS) that details the processes for registering users, issuing certificates, renewing certificates and revoking certificates. The CPS is normally published on the certificate authority's website.

20 Certificates often contain additional information that identifies an individual as a member of a particular organization and perhaps the role that they play in the organization. For example, the certificate may identifying the certificate holder as being either an employee of a
25 company or a customer or subcontractor or supplier of the

company. The policies determining who is eligible to hold a certificate are therefore important if individuals and organizations are to rely upon this information. These policies govern the overall operation of the certificate authority.

In other disadvantageous PKI, every time a user needs a digital certificate, it is almost as if the user has never received any previous certificates. That is, the user needs to authenticate his or her identity all over again. Since these other PKI's use manual processing for authenticating the identity of the user, this approach tends to be labor-intensive, thereby resulting in high costs for obtaining digital certificates in that every subsequent digital certificate is just as expensive to issue as the first certificate.

SUMMARY OF THE INVENTION

An object of the present invention is to obtain an initial digital certificate for a user and then use this initial certificate to authenticate the user's identity for all subsequent certificate processing.

Another object of the present invention is to automatically obtain a second certificate for user using a first certificate by accessing a server platform using a user's server and the first certificate of the user to create a connection that authenticates both the user's server

identity via a server certificate of the user server and the user's identity via the users for certificate. A secure data channel is created between the server platform and the user server and a request for the second certificate is forwarded
5 by the user from the user server to the server platform. The server platform then generates the second certificate without requiring any manual intervention by an enterprise officer.

The first certificate may be a signature certificate while the second certificate may be an encryption certificate.

10 The first certificate may be an expiring signature certificate while the second certificate may be a replacement signature certificate.

The first certificate may be a signature certificate while the second certificate may be a replacement encryption
15 certificate to replace an expiring encryption certificate.

The first certificate may be a signature certificate while the second signature certificate may be one of either the user's current encryption certificate or an expired encryption certificate of the user.

20 BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and a better understanding of the present invention will become apparent from the following detailed description of example embodiments and the claims when read in connection with the accompanying drawings, all form a part of
25 the disclosure of this invention. While the foregoing and

following written and illustrated disclosure focuses on disclosing example embodiments of the invention, it should be clearly understood that the same as by way of illustration and example only and the invention is not limited thereto. The
5 spirit and scope of the present invention are limited only by the terms of the appended claims.

The following represents a brief description of the drawings, wherein:

Figure 1 is a block diagram illustrating an exemplary
10 architecture of a network in which the PKI processes of the present invention may be practiced.

Figure 2 is a partial block diagram illustrating the steps performed by a manual technique for generating a signature certificate.

15 Figure 3 is a block diagram illustrating an example of obtaining an encryption certificate in accordance with a present invention.

Figure 4 is a block diagram illustrating an example of replacing an expiring signature certificate in accordance with
20 the present invention.

Figure 5 is a block diagram illustrating an example of replacing an expiring encryption certificate in accordance with the present invention.

Figure 6 is a block diagram illustrating the steps performed by a manual technique for user recovery of encryption certificates.

Figure 7 is a block diagram illustrating an example of user recovery of encryption certificates in accordance with the present invention.

DETAILED DESCRIPTION

Before beginning a detailed description of the subject invention, mention of the following is in order. When appropriate, like reference numerals and characters may be used to designate identical, corresponding, or similar components in differing drawing figures. Furthermore, in the detailed description to follow, example sizes/models/values/ranges may be given, although the present invention is not limited thereto. Lastly, well-known components and connections have not been shown within the drawing figures for simplicity of illustration and discussion and so is not to obscure the invention.

Fig. 1 illustrates an exemplary architecture of a network 100 in which the Public Key Infrastructure (P.K.I) processes of the present invention may be practiced. However, it should be understood that the present invention is not limited to the network 100 of FIG. 1. The network 100 includes data entry 102, which performs a data entry function for authoritative database 104, which is resident on the server platform 106. A

server platform 106 is referred to in this description, but it should be understood that the present invention is not limited to any particular server architecture. The server platform 106 may be, without limitation, a UNIX or Windows NT server.

5 The authoritative database 104 contains information about members of the group or enterprise for which PKI services in accordance with the present invention are performed. The present invention is not limited by the structure of the group enterprise for which information is stored in the

10 authoritative database 104. The authoritative database 104 information includes, without limitation, the name, address, telephone numbers, manager's name, employee identification, etc., of the members of the group or enterprise. Directory 108 has the structure of the database but is optimized for
15 fast look-up of information stored therein rather than fast data entry. The data in the directory 108 is not changed frequently but is required to be accessed rapidly and functions on-line as a fast phone book, containing reference information about the members of the group or enterprise

20 stored in the authoritative database 104. Certificate authority 110 is off-the-shelf software executed on server platform 106, providing storage of certificates and related information used by the present invention as described in more detail hereinafter. Registration authority 112 is also off-
25 the-shelf software executable on server platform 106 regarding

registration performed by the present invention as described in more detail hereinafter. Key authority 114 is also off-the-shelf server software which is executable on server platform 106 for recovering keys from members of the group or enterprise as described in more detail hereinafter. Windows 2000 Domain CA 116 may use certificates provided by the present invention for a single sign-on to the network 100 of FIG. 1. Legacy server 118 executes legacy application programs 120. The legacy server may be, without limitation, a main frame, mini-computer, workstation, or other server hosting legacy software applications that are designed to be run on PKI processes in accordance with the present invention. The legacy applications 120 are accessible on the client side by a custom client 128 such as an emulator or custom database Graphic User Interface (GUI). Examples of emulators are terminal emulators of an IBM 3270 or terminal emulators of a vt 100. Registration web page 122, which may be one or more pages, functions as the user interface to the network 100 of Fig. 1. Web server 124 is a software application which serves Web Pages, such as Web Page 122 or other HTML outputs, to a web browser client which may be, without limitation, Apache or a Microsoft Internet Information Server. Web browser 126 is resident on client platform 128 which may be any user computer. Web browser 126 is a client software application for browsing web pages such as but not limited to HTML or XML

protocols or other protocols. The Web browser 126 is programmed to operate with PKI certificates issued by the certificate authority 110. Examples of web browsers which have this capability are Netscape Navigator and the Microsoft Internet Explorer. The token 130 is a smart card, USB (United Serial Bus), or other hardware token capable of generating, storing, and using PKI certificates. A user 132 is a person using the network 100. A user 132 transitions through a number of states which include a new user, current user, and a former user who no longer is a member of the group or enterprise. The network 100 is described with reference to two levels of security, but the number of the levels of security is not a limitation of the present invention, with each level corresponding to a different security requirement. The level 1 search engine 134 is a search engine which is permitted to search through the network 100 but is allowed access to only level 1 data, which is the lowest level of security and may be, without limitation, data which is freely distributable. Level 2 data may be considered to be proprietary. Level 2 search engine 136 is a search engine which is allowed to search through both level 1 and level 2 data. A level N search engine (not illustrated) is a search engine which is allowed to search through servers possessing data levels 1 through N. A secured level server with level 1 data 138 is a Web server containing only level 1 data, which

is secured so that users must have level 1 access (at least) to access the server. A secured Web server with level 2 data 140 is a Web server that contains level 2 data which has been secured so that users must have level 2 access, with level 2 5 users having access to both level 1 and level 2 servers. A secured Web server with level N data (not illustrated) is a Web server that contains level N data which is accessible by a user with level N or above access. VPN Extranet 142 is a software application which functions as a network gateway 10 which, as illustrated, may be either to legacy server 118 and legacy application 120 or to an external network such as the Internet. Personal registration authority 144 is a person who is in charge of revocation of members from the network 100. Personal registration authority 146 is a person who is in 15 charge of registration of members in the network 100. Personal recovery approval 148 is a person in charge of obtaining recovery of certificates. A Recovery Agent 150 is a person who performs recovery of certificates and may only recover a certificate if the certificate has first been 20 designated as recoverable by another person. Personal role approval 152 is a person who approves different role functions within the network 100. A Web server administrator is in charge of various web functions in the network 100.

Figure 2 illustrates a partial block diagram of a network 25 bearing some features in common with that of the network 100

of Figure 1. Figure 2 has been provided to enable the discussion of a manual technique for generating a signature certificate. Elements in Figure 2 which correspond to those of Figure 1 have been labeled with the same designation numbers. Note that the level 1 and level 2 search engines 134 and 136 of Figure 1 have been replaced by the single search engine 270 and the secured Web servers 138 and 140 of Figure 1 have been replaced by the single secured Web server 280.

In step 1 of Figure 2, the user 132 physically presents a photo ID to the Local Registration Authority Officer (LRAO) 230. In step 2, the LRAO 230 then uses software contained in the local registration authority 250 to signal the registration authority 112 to register the new user 132. In step 3, a public/private key pair is generated by either the local registration authority 250 software or the registration authority 112 software, depending on the products chosen and depending on how they've been configured. The public key is sent to the certificate authority 110 to be signed, thereby generating a "certificate". In step 4, a backup copy of the private key may also optionally be sent to the key recovery authority 114. In step 5, the user's certificate is forwarded to the local registration authority 250. In step 6, the LRAO 230 copies the certificate (including the private key) onto a floppy disk or hardware token 130 or other storage medium and then physically hands the stored certificate and private key

to the user 132. The LRAO 230 must manually mark the database or log with the pedigree of the certificate.

In other disadvantageous PKI's, replacing an expiring signature certificate is unfortunately similar to the process
5 illustrated in Figure 2 for generating a signature certificate. That is, referring to Figure 2, in step 1, the user 132 presents a photo ID to the LRAO 230 in order to authenticate the identity of the user 132. Then, in step 2, the LRAO 230 uses LRA 250 software to signal the RA 112 to
10 create a new signature certificate for the user 132. In step 3, the public/private key pair is generated by either the LRA 250 or the RA 112 software, depending on the products chosen and depending on how they have been configured. The public key is sent to the CA 110 to be signed, thereby generating a
15 signature certificate. Optionally, depending on the products chosen and depending on how they have been configured, a backup copy of the private key may also be sent to the KRA 114. In step 5, the user's signature certificate is provided to the LRA 250. In step 6, the LRAO 230 copies the signature
20 certificate including the private key onto a floppy disk, hardware token, or other storage medium. The LRAO 230 then hands the signature certificate and private key to the user 132. Thus, replacing an expiring signature certificate requires the same amount of time and expense as providing the
25 signature certificate initially.

Referring to Figure 3, it is assumed that the user 132 is already listed in the directory 108 and already has a signature certificate. In step 1, a user 132 accesses the Registration Web Page 122 contained in the Registration Web server 124 using his or her signature certificate. The user's signature certificate is used to create a connection that authenticates both the server identity via a server certificate and the user's identity via the user's signature certificate. Any encryption scheme is then used to create a secure data channel between the Registration Web server 124 and the user 132. The user 132 then requests an encryption certificate from the Registration Web server 124. In step 2, the Registration Web server 124 queries the directory 108 to ensure that the user is still a member of the enterprise and to ensure that the user does not already have an encryption certificate, (since the user cannot have two concurrently valid encryption certificates). In step 3, the Registration Web server 124 signals the RA (Registration Authority) 112 to generate a private/public key pair. In step 4, the RA 112 uses the encrypted channel to send the private key back to the user 132 to either directly or via the Registration Web server 124. In step 5, the RA 112 sends the public key to the CA (Certificate Authority) 110 to be signed by the CA 110. In step 6, a backup copy of the private key may be sent to the KRA (Key Recovery Authority) 114. In step 7, the CA 110 signs

the public key and sends the signed certificate to the directory 108. Note that no enterprise officer was needed to obtain the encryption certificate since the "chain of trust" was used to authenticate the user via the user's signature certificate so as to obtain the encryption certificate.

An example of replacing an expiring signature certificate in accordance with the present invention will now be explained with reference to Figure 4. In step 1, a user 132 attempts to access a server 140, for example. In step 2, the server 140 requests the user's signature to authenticate the user's identity. In step 3, the user 132 presents a signature to the server 140 and in step 4, the server 140 queries the directory 108 to verify that the user 132 is allowed access to the server 140. In step 5, the directory 108 responds with a yes or no answer. If the answer is yes, then the user 132 is granted access to the server 140. In step 6, the server 140 also checks the expiration date of the user's signature certificate. If the expiration date is near, for example, within one month, then the server 140 redirects the user 132 to the Certificate Renewal Web Page 122 on the Registration Web Server 124.

In step 7, the user 132 attempts access to the Registration Web Server 124. It is to be noted that the Registration Web Server 124 is normally set up so as not to allow a user to replace an existing signature certificate

unless the existing signature certificate of the user is near its expiration date. Furthermore, if the pedigree of a user's signature certificate has been tracked, different users may access different registration Web pages on the Registration Web Server 124, depending on what level of signature certificate they possess. That is, a user with a level 2 certificate may access a registration Web Page that can be accessed only by holders of level 2 certificates.

In step 8, the Registration Web Server 124 requests the user's signature so as to authenticate the user identity and in step 9, the user 132 presents the signature to the Server 124. In step 10, the Server 124 queries the directory 108 to verify that the user 132 is allowed to access the Registration Web Server 124 and in step 11, the directory 108 responds with a yes or no answer. If the answer is yes, then the user 132 is granted access to the Server 124 and the user 132 requests replacement or renewal of the signature certificate. The subsequent steps include the Registration Web Server 124 signaling the RA 112 to re-register the user 132 and the RA 112 signaling the Web browser 126 on the client platform 128 to generate a private/public key pair and the public key is then sent to the CA 110 to be digitally signed and the signed certificate with public key is then sent from the CA 110 to the directory 108. A copy of the public key may also

optionally be sent back to the Web browser 126 from the CA 110.

Note that in the above-noted procedure, it was not necessary for the user 132 to come in face-to-face contact with the LRAO 230 nor was it necessary for the LRAO 230 to be involved in the replacement of the expiring signature certificate. Thus, the above-noted procedure is much quicker and far cheaper than that of the manual procedure required by other disadvantageous PKIs.

In other disadvantageous PKI's, replacing an expiring encryption certificate is the same as the process noted above with regard to replacing an expiring signature certificate in earlier PKI's. That is, it is necessary for the LRAO to be involved with the user to replace a user's expiring encryption certificate. Accordingly, replacing a user's expiring encryption certificate in earlier PKIs required the same amount of time and expense as providing the encryption certificate initially.

On the other hand, replacing an expiring encryption certificate in accordance with the present invention is considerably simpler and less expensive since no intervention by an LRAO is necessary.

An example of replacing an expiring encryption certificate in accordance with the present invention will now be explained with reference to Figure 5. In step 1, a user

132 accesses the Registration Web Server 124 to view the
Registration Web Page 122 using his or her signature
certificate. The user's signature certificate is used to
create a connection that authenticates both the server
5 identity via a server certificate and the user's identity via
the user's signature certificate. Any commonly used
encryption scheme may be used to create a secure data channel
between the Web Server 124 and the user 132. The user 132
requests an encryption certificate from the Registration Web
10 Server 124. In step 2, the Registration Web Server queries
the directory 108 to insure that the user 132 is still a valid
member of the enterprise. In step 3, the user 132 requests
the Registration Web Server 124 to revoke the existing
encryption certificate. This is necessary in view of the
15 assumption that a user may not have two concurrently valid
encryption certificates. In step 4, the Registration Web
Server 124 signals the directory 108 that the user's
encryption certificate has been revoked and in step 5, the
Registration Web Server 124 signals the CA 110 that the user's
20 encryption certificate has been revoked. In step 6, the
Registration Web Server 124 signals the RA 112 to generate a
private/public key pair and in step 7 the RA 112 uses an
encrypted channel to send the private key back to the user 132
either directly or via the Registration Web Server 124. In
25 step 8, the RA 112 send the public key to the CA 110 to be

signed by the CA and in step 9, the CA 110 signs the public key and sends the signed public key and the signed certificate to the directory 108. A backup copy of the private key may also be sent to the Key Recovery Authority 114.

- 5 Recovering old copies of now-expired encryption certificates in other disadvantageous PKIs is expensive in that the recovery must be performed manually since other PKIs do not take advantage of the fact that the recovery process can be automated by exploiting the strong authentication of
10 the user's signature certificate.

 Figure 6 illustrates the manual user recovery of encryption certificates in accordance with other disadvantageous PKIs. Namely, a user 132 approaches an enterprise officer, such as an LRAO 230 as shown in step 1a or
15 a KRO (Key Recovery Officer) 500 as shown in step 1b. The choice of enterprise officer depends on the specific PKI. For the purpose of discussion, it is assumed that the LRAO 230 is the chosen enterprise officer. In step 2, the LRAO 230 uses LRA 250 software to signal the KRA 114 to recover a copy of
20 the old encryption certificate for the user. The user's certificate is provided to the LRA 250 in step 3. In step 4, the LRAO 230 copies the certificate onto a floppy disk, hardware token, or other storage medium and then hands the certificate to the user 132.

Figure 7 illustrates an example of user recovery of encryption certificates in accordance with the present invention. It is assumed that the user 132 already exists in the directory 108 and it is also assumed that the user has a signature certificate and an encryption certificate.

In step 1, the user 132 accesses the KRA 114 via the Registration Web Server 124 using his or her signature certificate. The signature certificate is used to create a connection to the KRA 114 that authenticates both the server identity via a server certificate and the user's identity via the user's signature certificate. Any encryption scheme may be used to create a secure data channel between the server and the user. In step 2, the user 132 requests recovery of an encryption certificate from the KRA 114. The user 132 can either recover his or her current encryption certificate or an expired encryption certificate of the user 132. The KRA 114 uses the secure channel to deliver the requested encryption certificate to the user 132. In this fashion, the user 132 can recover both current and expired encryption certificates without requiring the manual intervention by an enterprise officer needed in other disadvantageous PKIs.

Thus, in accordance with the present invention, a secure manual procedure may be used to issue an initial digital certificate to a user and then, that initial certificate may be used to authenticate the user's identity for also

subsequent certificate processing including but not limited to obtaining, replacing, and recovering certificates.

If the user already processes a signature certificate, the signature certificate can be used to strongly authenticate the user's identity and to encrypt a transmission for one particular purpose, namely, to create a onetime secure channel via which the encryption certificate's private key can be exchanged between the user and a KRA.

A secure channel is necessary so that the encryption certificate's private key will not be compromised. However, since a secure channel can not be realized via the encryption certificate since the encryption certificate has not been generating yet, the signature certificate is used to encrypt.

Stated simply, in accordance with the present invention, the initial signature certificate may be used as a mechanism for establishing a "chain of trust" that can be used to obtain all other certificates.

This concludes the description of the example embodiments. Although the present invention has been described with reference to a number of illustrative embodiments thereof, it should be understood that numerous other modifications and embodiments can be devised by those skilled of the art that will fall within the spirit and scope of the principles of this invention. More particularly, reasonable variations and modifications are possible in the

component parts and/or arrangements of the subject combination arrangement within the scope of the foregoing disclosure, the drawings, and the appended claims without departing from the spirit of the invention. In addition to variations and

5 modifications in the component parts and/or arrangements, alternative uses will also be apparent to those skilled of the art.

For example, the particular arrangement of elements illustrated in the drawing figures is by no means unique.

10 Furthermore, the various server platforms may either be combined or separated to suit specific needs. Still furthermore, one enterprise officer may serve more than one function or vice versa.

15 What is claimed is:

CLAIMS:

1 1. A method of automatically obtaining a second
2 certificate for a user using a first certificate, the method
3 comprising:

4 accessing a registration server using a user's
5 server and the first certificate of the user to create a
6 connection that authenticates both the user's server identity
7 via a server certificate of the user server and the user's
8 identity via the user's first certificate;

9 creating a secure data channel between the
10 registration server and the user server;

11 forwarding a request for the second certificate from
12 the user server to the registration server;

13 determining in the registration server that the user
14 is entitled to the second certificate;

15 forwarding a request from the registration server to
16 an authority to generate a private/public key pair;

17 sending the private key to the user from the
18 authority via the secure data channel;

19 sending the public key from the authority to another
20 authority to be signed; and

21 forwarding the second certificate from the another
22 authority to a directory.

1 **2.** The method of claim **1**, further comprising sending a
2 backup copy of the private key from the authority to a key
3 recovery authority.

1 **3.** The method of claim **1**, wherein the first certificate
2 comprises a signature certificate.

1 **4.** The method of claim **1**, wherein the second
2 certificate comprises an encryption certificate.

1 **5.** The method of claim **1**, wherein the first certificate
2 comprises an expiring signature certificate and the second
3 certificate comprises a replacement signature certificate.

1 **6.** The method of claim **1**, wherein the first certificate
2 comprises a signature certificate and the second certificate
3 comprises a replacement encryption certificate.

1 **7.** The method of claim **1**, wherein the first certificate
2 comprises a signature certificate and the second certificate
3 comprises one of either the user's current encryption
4 certificate or an expired encryption certificate of the user.

1 **8.** A method of automatically obtaining a second
2 certificate for a user using a first certificate, the method
3 comprising:
4 accessing a server platform using a user's server
5 and the first certificate of the user to create a connection
6 that authenticates both the user's server identity via a
7 server certificate of the user server and the user's identity
8 via the user's first certificate;
9 creating a secure data channel between the server
10 platform and the user server;
11 forwarding a request for the second certificate from
12 the user server to the server platform; and
13 generating at the server platform the second
14 certificate.

1 **11.** The method of claim **8**, wherein the first certificate
2 comprises a signature certificate.

1 **12.** The method of claim **8**, wherein the second
2 certificate comprises an encryption certificate.

1 **13.** The method of claim **8**, wherein the first certificate
2 comprises an expiring signature certificate and the second
3 certificate comprises a replacement signature certificate.

1 **14.** The method of claim **8**, wherein the first certificate
2 comprises a signature certificate and the second certificate
3 comprises a replacement encryption certificate.

1 **15.** The method of claim **8**, wherein the first certificate
2 comprises a signature certificate and the second certificate
3 comprises one of either the user's current encryption
4 certificate or an expired encryption certificate of the user.

1 **16.** An apparatus for automatically obtaining a second
2 certificate for a user using a first certificate, the
3 apparatus comprising:

4 a user server and a registration server, the user
5 server accessing the registration server using the first
6 certificate of the user to create a connection that
7 authenticates both the user's server identity via a server
8 certificate of the user server and the user's identity via the
9 user's first certificate;

10 a secure data channel, the secure data channel being
11 disposed between the registration server and the user server,
12 the user server forwarding a request for the second
13 certificate to the registration server through the secure data
14 channel;

15 a first authority, the registration server
16 determining that the user is entitled to the second

17 certificate and forwarding a request to the first authority to
 18 generate a private/public key pair, the first authority
 19 sending the private key to the user via the secure data
 20 channel;

21 a second authority, the first authority sending the
 22 public key to the second authority to be signed; and

23 a directory, the second authority forwarding the
 24 second certificate to the directory.

1 17. The apparatus of claim 16, wherein the first
 2 certificate comprises a signature certificate.

1 18. The apparatus of claim 16, wherein the second
 2 certificate comprises an encryption certificate.

1 19. The apparatus of claim 16, wherein the first
 2 certificate comprises an expiring signature certificate and
 3 the second certificate comprises a replacement signature
 4 certificate.

1 20. The apparatus of claim 16, wherein the first
 2 certificate comprises a signature certificate and the second
 3 certificate comprises a replacement encryption certificate.

1 **21.** The apparatus of claim **16**, wherein the first
2 certificate comprises a signature certificate and the second
3 certificate comprises one of the user's current encryption
4 certificate and an expired encryption certificate of the user.

1 **22.** An apparatus for automatically obtaining a second
2 certificate for a user using a first certificate, the
3 apparatus comprising:

4 a user server and a server platform, the user server
5 accessing the server platform using the first certificate of
6 the user to create a connection that authenticates both the
7 user's server identity via a server certificate of the user
8 server and the user's identity via the user's first
9 certificate;

10 a secure data channel, the secure data channel being
11 disposed between the server platform and the user server;

12 the user server forwarding a request for the second
13 certificate to the server platform; and

14 the server platform generating the second
15 certificate.

1 **23.** The apparatus of claim **22**, wherein the first
2 certificate comprises a signature certificate.

1 **24.** The apparatus of claim **22**, wherein the second
2 certificate comprises an encryption certificate.

1 **25.** The apparatus of claim **22**, wherein the first
2 certificate comprises an expiring signature certificate and
3 the second certificate comprises a replacement signature
4 certificate.

1 **26.** The apparatus of claim **22**, wherein the first
2 certificate comprises a signature certificate and the second
3 certificate comprises a replacement encryption certificate.

1 **27.** The apparatus of claim **22**, wherein the first
2 certificate comprises a signature certificate and the second
3 certificate comprises one of either the user's current
4 encryption certificate or an expired encryption certificate of
5 the user.

CHAIN OF TRUST PROCESSINGABSTRACT

A technique for automatically obtaining a second certificate for a user using a first certificate includes
10 accessing a server platform using a user's server and the first certificate of the user to create a connection that authenticates both the user's server identity via a server certificate of the user server and the user's identity via the user's first certificate. A secure data channel is then
15 created between the server platform and the user platform. A request for the second certificate is forwarded by the user from the user server to the server platform and the server platform then generates the second certificate. The first certificate may be a signature certificate and the second certificate may be an encryption certificate. The first
20 certificate may be an expiring signature certificate and the second certificate may be a replacement signature certificate. The first certificate may be a signature certificate and the second certificate may be a replacement encryption certificate
25 to replace an expiring encryption certificate. The first certificate may be a signature certificate and the second certificate may be one of either the user's current encryption certificate or an expired encryption certificate of the user. Thus, the first certificate may be used as a mechanism for
30 establishing a "chain of trust" that can be used to obtain all

other certificates without requiring the manual intervention of an enterprise officer, thereby considerably reducing the time and expense of obtaining additional certificates for a user.

CONFIDENTIAL

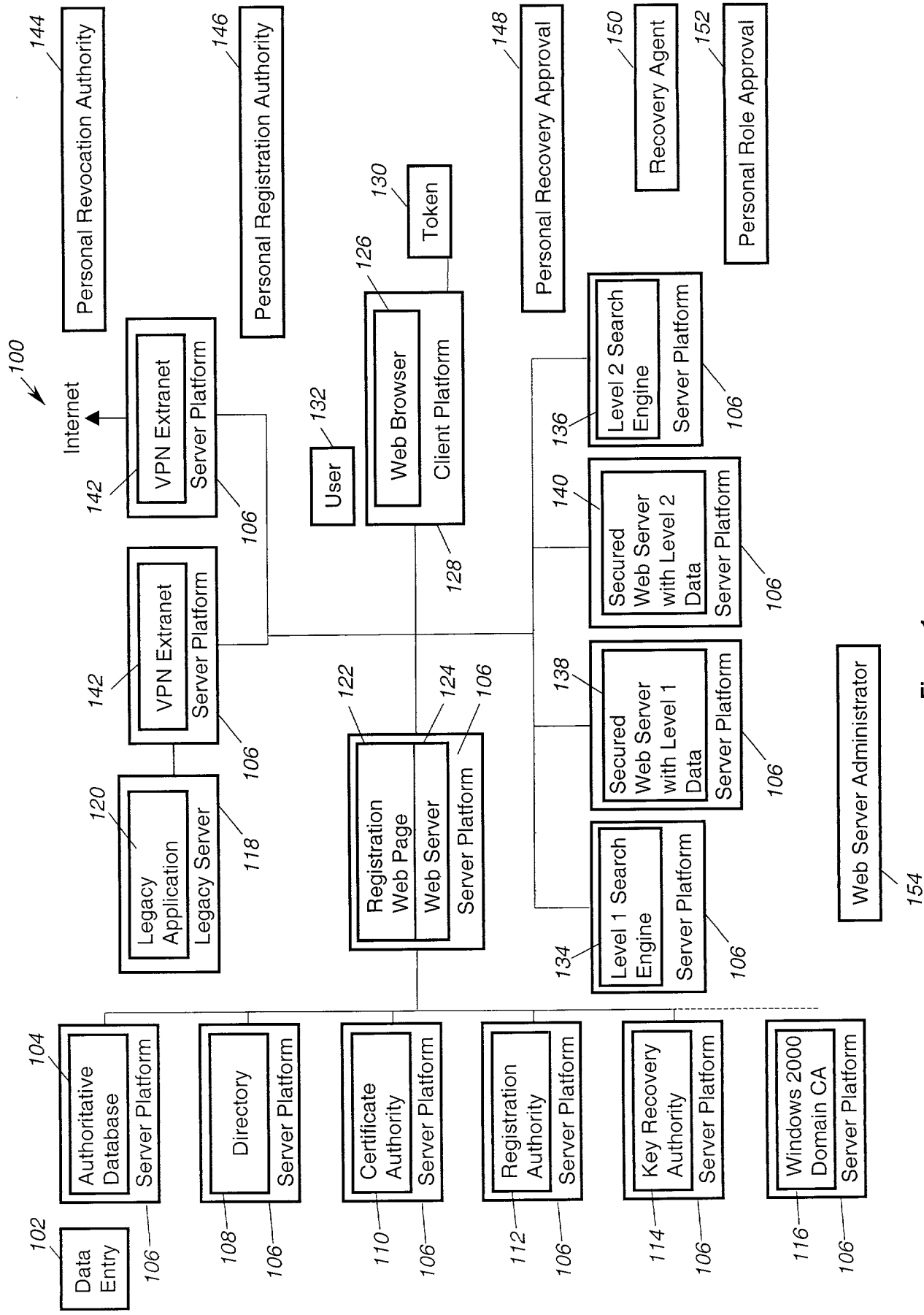


Figure 1

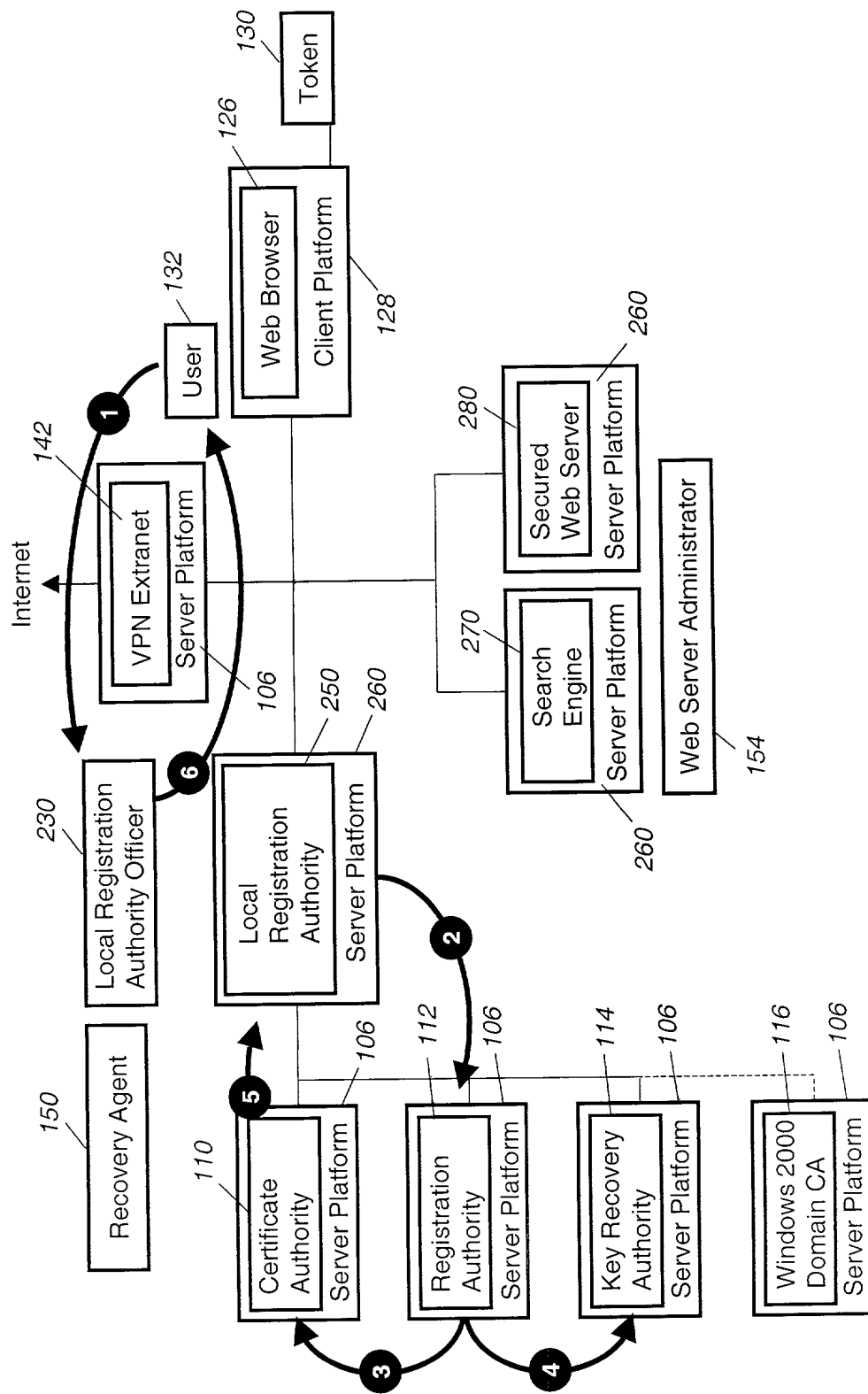


Figure 2

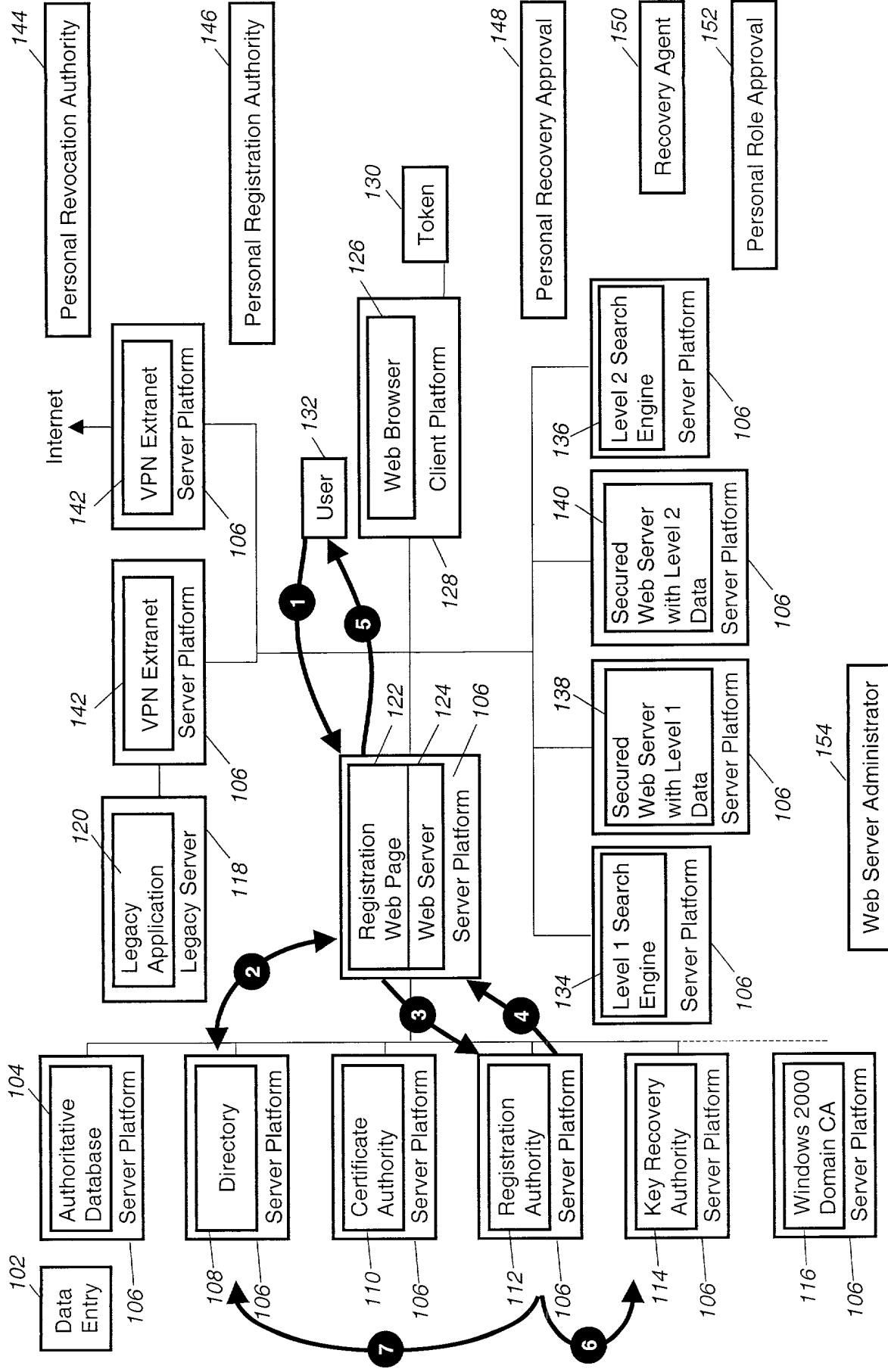


Figure 3

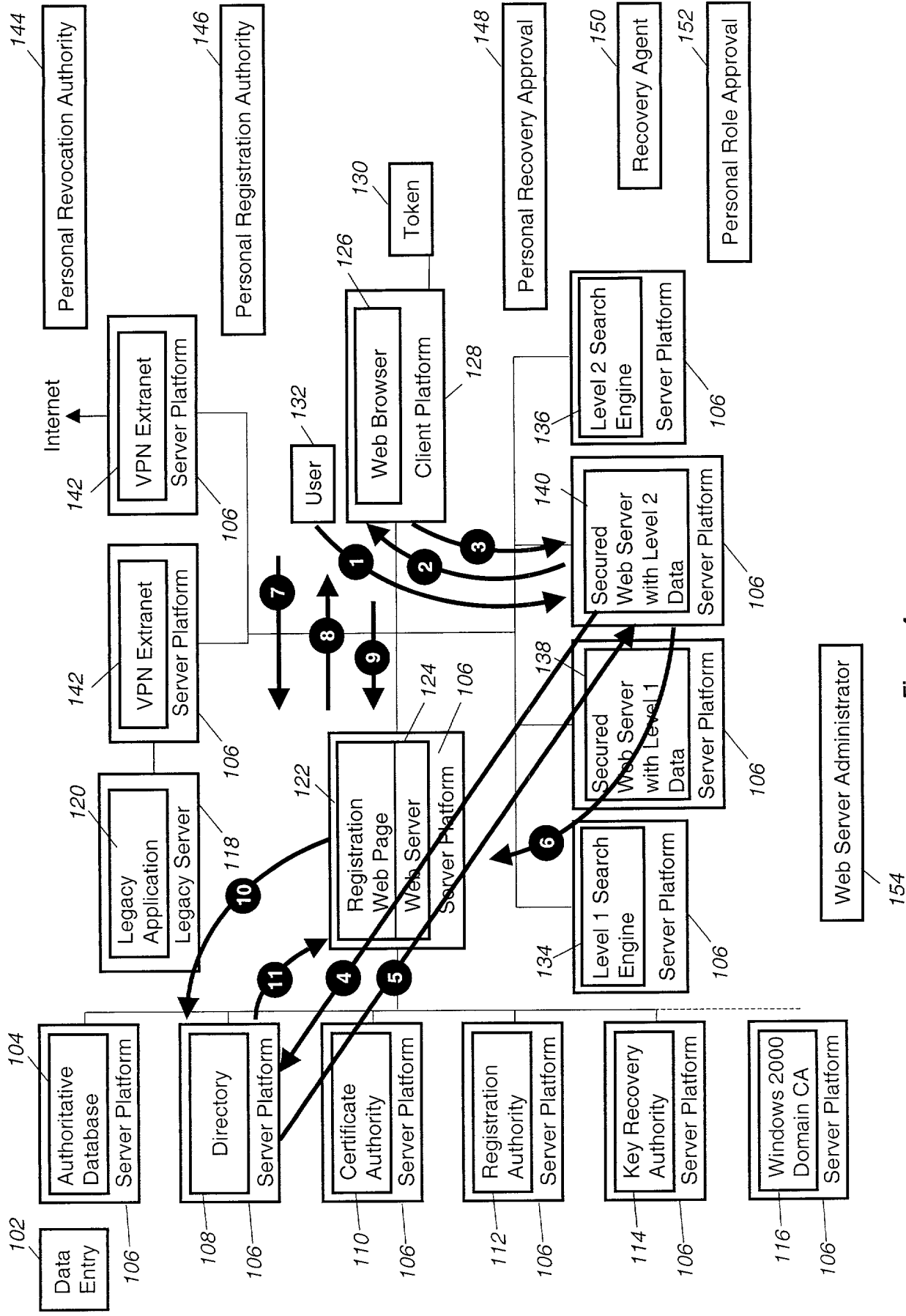


Figure 4

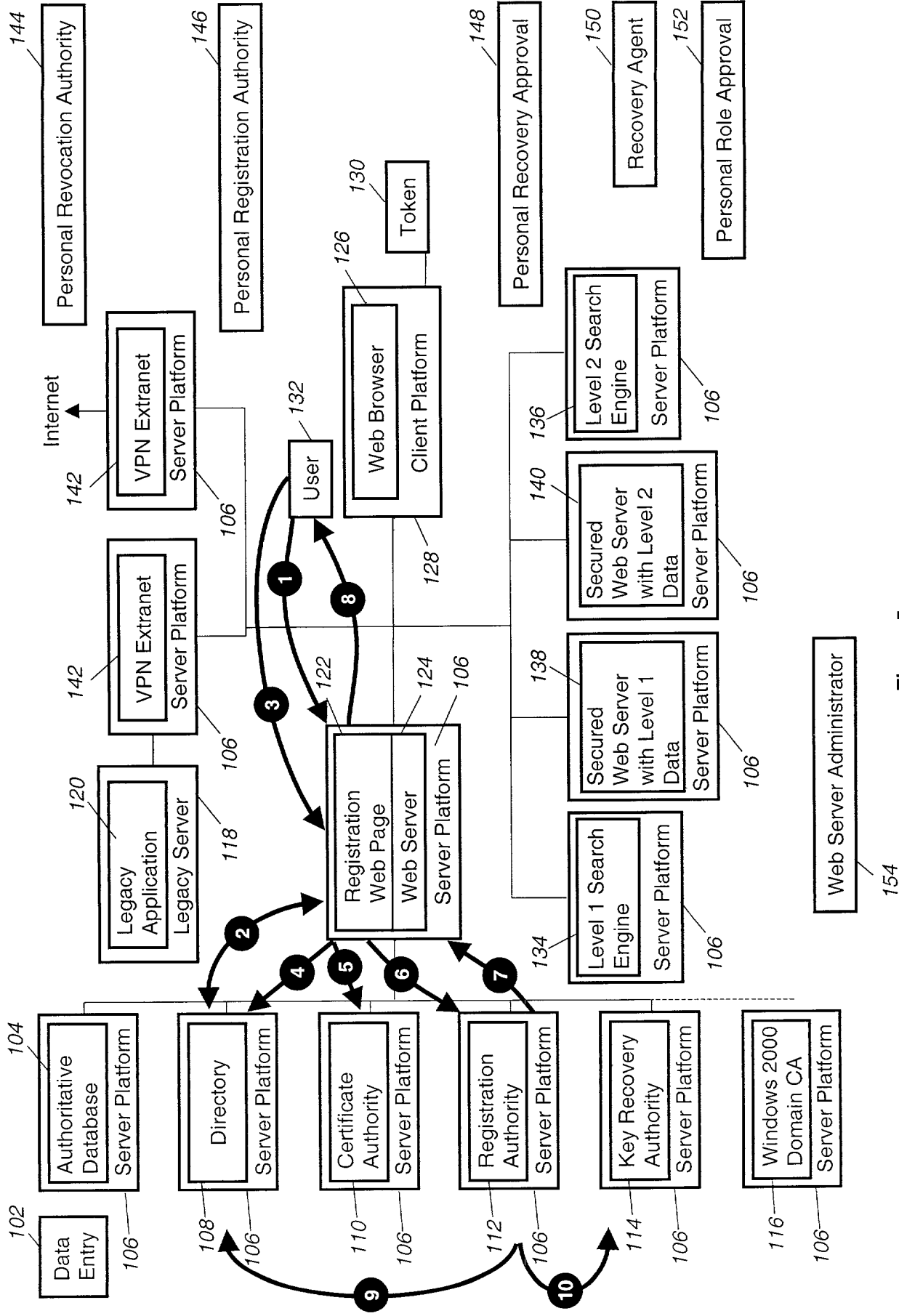


Figure 5

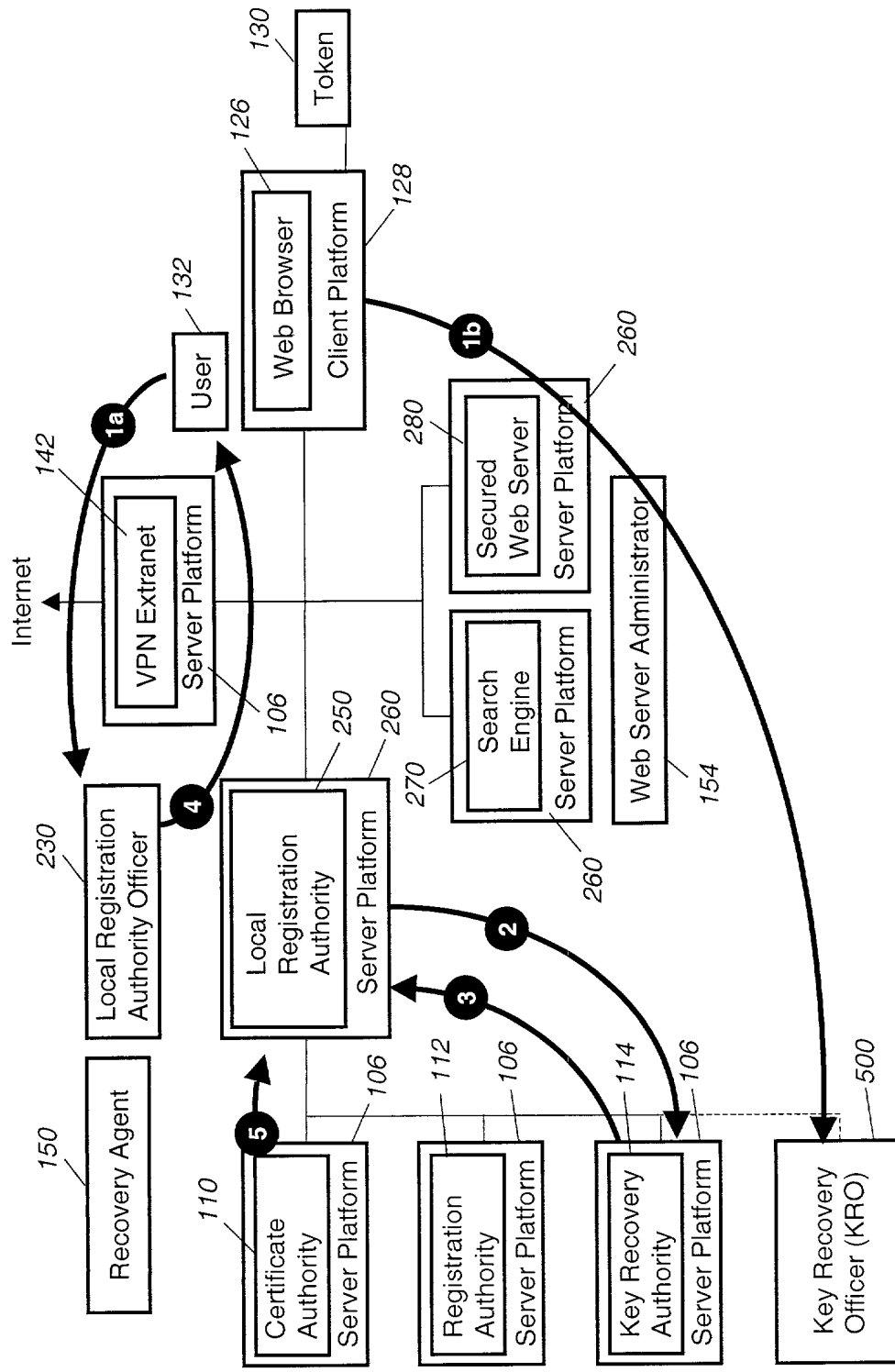


Figure 6

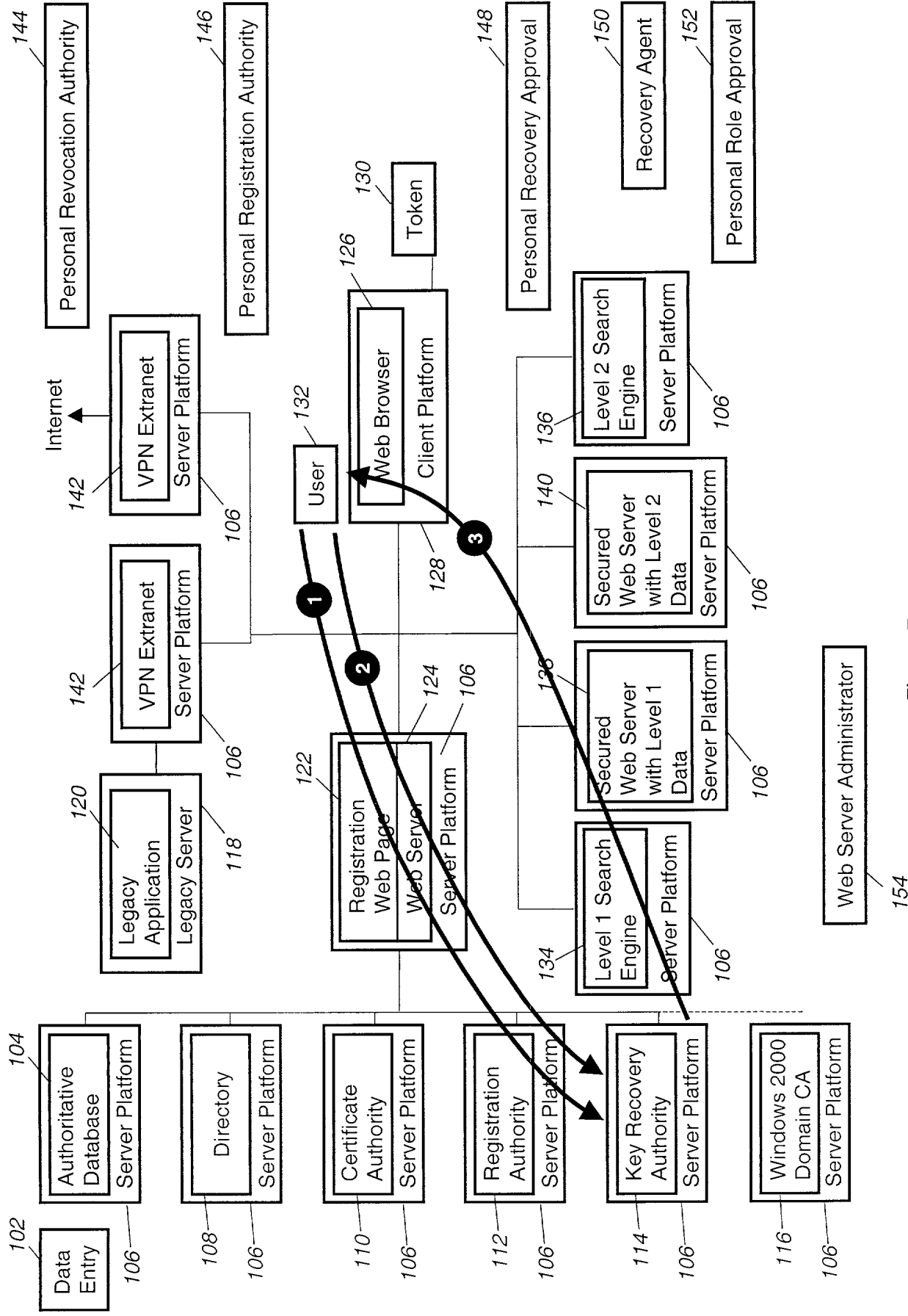


Figure 7

Docket No. 15-0231

DECLARATION FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled CHAIN OF TRUST PROCESSING the specification of which

_____ is attached hereto

_____ was filed on _____ as Application
Serial No. _____ and was amended on
_____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

Priority Claimed

<u>NONE</u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>
(Number)	(Country)	(Day/Mo./Yr. Filed)	Yes	No

Docket No. 15-0231

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

<u>60/229,336</u>	<u>USA</u>	<u>September 1, 2000</u>	<u>Pending</u>
(Number)	(Country)	(Day/Mo./Yr. Filed)	(Status)

I hereby appoint as principal attorneys:

Robert W. Keller, Reg. No. 25,347
Michael S. Yatsko, Reg. No. 28,135
Connie M. Thousand, Reg. No. 43,191
Donald E. Stout, Reg. No. 26,422

Each with full power to prosecute this application, to transact all business in the United States Patent and Trademark Office connected therewith, and to appoint and revoke associate and substitute associate attorneys.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Address all telephone calls to: (310) 812-4910

Address all correspondence to: PATENT COUNSEL
TRW Inc.
Space & Electronics Group
One Space Park, E2/6051
Redondo Beach, California 90278

Full name of sole or first inventor Kenneth W. Aull

Inventor's signature _____ Date: _____

Residence Fairfax, Virginia

Citizenship United States

Post Office Address 5364 Lake Normandy Court, Fairfax, VA 22030